Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

1. (Currently Amended) A layer 2 network access device for providing network security, comprising: a plurality of input ports;

   a switching fabric in the layer 2 network access device for routing data received on the ~~said~~ plurality of input ports to at least one output port; and

   control logic in the layer 2 network access device adapted to authenticate a physical address of a user device coupled to one of the ~~said~~ plurality of input ports, to authenticate user information provided by a user of the ~~said~~ user device only if the ~~said~~ physical address is valid, and to restrict access to the ~~said~~ one of the ~~said~~ plurality of input ports in accordance with a user policy associated with the ~~said~~ user information only if the ~~said~~ user information is valid.

2. (Currently Amended) The network access device of claim 1, wherein the ~~said~~ physical address comprises a Media Access Control (MAC) address.

3. (Currently Amended) The network access device of claim 1, wherein the ~~said~~ control logic is adapted to authenticate the ~~said~~ user information in accordance with an IEEE 802.1x protocol.

4. (Currently Amended) The network access device of claim 1, wherein the ~~said~~ user policy identifies an access control list.

5. (Currently Amended) The network access device of claim 1, wherein the ~~said~~ user policy includes an access control list.

6. (Currently Amended) The network access device of claim 1, wherein the ~~said~~ user policy identifies a Media Access Control (MAC) address filter.

7. (Currently Amended) The network access device of claim 1, wherein the ~~said~~ user policy includes a Media Access Control (MAC) address filter.

8. (Currently Amended) The network access device of claim 1, wherein the ~~said~~ control logic is adapted to send the ~~said~~ user information to an authentication server and to receive an accept message from the ~~said~~ authentication server if the ~~said~~ user information is valid.

9. (Currently Amended) The network access device of claim 8, wherein the ~~said~~ authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

10. (Currently Amended) The network access device of claim 8, wherein the ~~said~~ accept message includes the ~~said~~ user policy.

11. (Currently Amended) The network access device of claim 1, wherein the ~~said~~ control logic is further adapted to assign the ~~said~~ one of the ~~said~~ plurality of input ports to a virtual local area network (ULAN) associated with the ~~said~~ user information if the ~~said~~ user information is valid.

12. (Currently Amended) The network access device of claim 11, wherein the ~~said~~ control logic is adapted to receive a message from an authentication server, wherein the ~~said~~ message comprises a VLAN identifier (ID) associated with the ~~said~~ user information, and to assign the ~~said~~ one of the ~~said~~ plurality of input ports to a ULAN associated with the ~~said~~ VLAN ID.

13. (Currently Amended) A method for providing network security, comprising:

authenticating in a layer 2 network access device a physical address of a user device coupled to a port of the network access device;

authenticating user information provided by a user of the ~~said~~ user device to the network access device only if the ~~said~~ physical address is valid; and

restricting access to the ~~said~~ port in accordance with a user policy associated with the ~~said~~ user information only if the ~~said~~ user information is valid.

14. (Currently Amended) The method of claim 13, wherein the ~~said~~ authenticating a physical address comprises authenticating a Media Access Control (MAC) address.

15. (Currently Amended) The method of claim 13, wherein the ~~said~~ authenticating the ~~said~~ user information comprises authenticating the ~~said~~ user information in accordance with an IEEE 802.1x protocol.

16. (Currently Amended) The method of claim 13, wherein the ~~said~~ restricting access comprises restricting access to the ~~said~~ one of the ~~said~~ plurality of input ports in accordance with an access control list.

17. (Currently Amended) The method of claim 13, wherein the ~~said~~ restricting access comprises restricting access to the ~~said~~ one of the ~~said~~ plurality of input ports in accordance with a Media Access Control (MAC) address filter.

18. (Currently Amended) The method of claim 13, wherein the ~~said~~ authenticating the ~~said~~ user information comprises:

sending the ~~said~~ user information to an authentication server; and receiving an accept message from the ~~said~~ authentication server if the ~~said~~ user information is valid.

19. (Currently Amended) The method of claim 18, wherein the ~~said~~ authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

20. (Currently Amended) The method of claim 18, wherein the ~~said~~ receiving an accept message comprises receiving an accept message that includes the ~~said~~ user policy.

21. (Currently Amended) The method of claim 13, further comprising:

assigning the ~~said~~ port to a virtual local area network (VLAN) associated with the ~~said~~ user information only if the ~~said~~ user information is valid.

22. (Currently Amended) The method of claim 21, wherein the ~~said~~ assigning the ~~said~~ port to a VLAN comprises:

receiving a message from an authentication server, wherein the ~~said~~ message comprises a VLAN identifier (ID) associated with the ~~said~~ user information; and

assigning the ~~said~~ port to a VLAN associated with the ~~said~~ VLAN ID.

23. (Currently Amended) A network system, comprising: a data communications network;

a layer 2 network access device coupled to the ~~said~~ data communications network; and

a user device coupled to a port of the ~~said~~ network access device;

wherein the ~~said~~ network access device is adapted to authenticate a physical address of the ~~said~~ user device, to authenticate user information provided by a user of the ~~said~~ user device only if the ~~said~~ physical address is valid, and to restrict access to the ~~said~~ port in accordance with a user policy associated with the ~~said~~ user information only if the ~~said~~ user information is valid.

24. (Currently Amended) The system of claim 23, wherein the ~~said~~ physical address comprises a Media Access Control (MAC) address.

25. (Currently Amended) The system of claim 23, wherein the ~~said~~ network access device is adapted to authenticate the ~~said~~ user information in accordance with an IEEE 802. lx protocol.

26. (Currently Amended) The system of claim 23, wherein the ~~said~~ user policy identifies an access control list.

27. (Currently Amended) The system of claim 23, wherein the ~~said~~ user policy includes an access control list.

28. (Currently Amended) The system of claim 23, wherein the ~~said~~ user policy identifies a Media Access Control (MAC) address filter.

29. (Currently Amended) The system of claim 23, wherein the ~~said~~ user policy includes a Media Access Control (MAC) address filter.

30. (Currently Amended) The system of claim 23, further comprising:

an authentication server coupled to the ~~said~~ data communications network;

wherein the ~~said~~ network access device is adapted to send the ~~said~~ user information to the ~~said~~ authentication server and to receive an accept message from the ~~said~~ authentication server if the ~~said~~ user information is valid.

31. (Currently Amended) The system of claim 30, wherein the ~~said~~ authentication server comprises a Remote Authentication Dial-In User Service (RADIUS) server.

32. (Currently Amended) The system of claim 30, wherein the ~~said~~ accept message includes the ~~said~~ user policy.

33. (Currently Amended) The system of claim 23, wherein the ~~said~~ network access device is further adapted to assign the ~~said~~ port to a virtual local area network (VLAN) associated with the ~~said~~ user information if the ~~said~~ user information is valid.

34. (Currently Amended) The system of claim 33, further comprising:

an authentication server coupled to the ~~said~~ data communications network;

wherein the ~~said~~ network access device is adapted to receive a message from the ~~said~~ authentication server, wherein the ~~said~~ message comprises a VLAN identifier (ID)

associated with the ~~said~~ user information, and to assign the ~~said~~ port to a VLAN associated with the ~~said~~ VLAN ID if the ~~said~~ user information is valid.

35. (Currently Amended) The network access device of claim 2 wherein the ~~said~~ control logic is further configured to:

if authentication of the ~~said~~ MAC address indicates the ~~said~~ MAC address is invalid,

drop packets from the ~~said~~ user device; or

disable the ~~said~~ port;

if authentication of the ~~said~~ user information indicates the ~~said~~ user information is invalid,

block all traffic on the ~~said~~ port except for packets related to a user authentication protocol;

if authentication of user information indicates the ~~said~~ user information is valid, determine whether the ~~said~~ user is associated with a VLAN supported by the ~~said~~ network access device;

if the ~~said~~ user is not associated with the ~~said~~ VLAN,

assign the ~~said~~ port to a port default VLAN; and

block all traffic on the ~~said~~ port except for packets related to the ~~said~~ user authentication protocol; and

if the ~~said~~ user is associated with the ~~said~~ VLAN,

assign the ~~said~~ port to the ~~said~~ VLAN associated with the ~~said~~ user; and

forward packets from the ~~said~~ user device.

36. (Currently Amended) The method of claim 14, further comprising:

if the ~~said~~ authenticating of the ~~said~~ MAC address indicates the ~~said~~ MAC address is invalid,

dropping packets from the ~~said~~ user device; or

disabling the ~~said~~ port;

if the ~~said~~ authenticating user information indicates the ~~said~~ user information is invalid,

blocking all traffic on the ~~said~~ port except for packets related to a user authentication protocol;

if the ~~said~~ authenticating user information indicates the ~~said~~ user information is valid,

determining whether the ~~said~~ user is associated with a VLAN supported by the ~~said~~ network access device;

if the ~~said~~ determining indicates the ~~said~~ user is not associated with the ~~said~~ VLAN,

assigning the ~~said~~ port to a port default VLAN; and

blocking all traffic on the ~~said~~ port except for packets related to the ~~said~~ user authentication protocol; and

if the ~~said~~ determining indicates the ~~said~~ user is associated with the ~~said~~ VLAN,

assigning the ~~said~~ port to the ~~said~~ VLAN associated with the ~~said~~ user; and

forwarding packets from the ~~said~~ user device.

37. (Currently Amended) The network system of claim 24 wherein the ~~said~~ network access device is further adapted to:

if authentication of the ~~said~~ MAC address indicates the ~~said~~ MAC address is invalid,

dropping packets from the ~~said~~ user device; or

disabling the ~~said~~ port;

if authentication of the ~~said~~ user information indicates the ~~said~~ user information is invalid,

block all traffic on the ~~said~~ port except for packets related to a user authentication protocol;

if authentication of user information indicates the ~~said~~ user information is valid, determine whether the ~~said~~ user is associated with a VLAN supported by the ~~said~~ network access device;

if the ~~said~~ user is not associated with the ~~said~~ VLAN,

assign the ~~said~~ port to a port default VLAN; and

block all traffic on the ~~said~~ port except for packets related to the ~~said~~ user authentication protocol; and

if the ~~said~~ user is associated with the ~~said~~ VLAN,

assign the ~~said~~ port to the ~~said~~ VLAN associated with the ~~said~~ user; and

forward packets from the ~~said~~ user device.

38. (Currently Amended) An apparatus for providing network security, comprising:

a plurality of input ports;

a switching fabric for routing data received on the ~~said~~ plurality of input ports to at least one output port; and

control logic adapted to:

authenticate a physical address of a user device coupled to one of the ~~said~~ plurality of input ports;

drop packets from the ~~said~~ user device if the ~~said~~ physical address is invalid;

authenticate user information provided by a user of the ~~said~~ user device only if the ~~said~~ physical address is valid;

if authentication of the ~~said~~ user information indicates the ~~said~~ user information is invalid, block all traffic on the ~~said~~ one of the ~~said~~ plurality of input ports except for packets related to a user authentication protocol;

if authentication of user information indicates the ~~said~~ user information is valid,

determine whether the ~~said~~ user is associated with a VLAN supported by the ~~said~~ apparatus by receiving a message from an authentication server, wherein the ~~said~~ message comprises a VLAN identifier (ID) associated with the ~~said~~ user information;

if the ~~said~~ user is not associated with the ~~said~~ VLAN,

assign the ~~said~~ one of the ~~said~~ plurality of input ports to a port default VLAN; and

block all traffic on the ~~said~~ one of the ~~said~~ plurality of input ports except for packets related to the ~~said~~ user authentication protocol; and

if the ~~said~~ user is associated with the ~~said~~ VLAN,

assign the ~~said~~ one of the ~~said~~ plurality of ports to the ~~said~~ VLAN associated with the ~~said~~ user; and

restrict access to the ~~said~~ one of the ~~said~~ plurality of input ports in accordance with a user policy associated with the ~~said~~ user information.

39. (Currently Amended) The apparatus of claim 38, wherein the ~~said~~ apparatus comprises a layer 2 network access device.

40. (Currently Amended) A method for providing network security, comprising:

authenticating a physical address of a user device coupled to a port of a network access device;

dropping packets from the ~~said~~ user device if the ~~said~~ physical address is invalid;

authenticating user information provided by a user of the ~~said~~ user device only if the ~~said~~ physical address is valid;

if the ~~said~~ authenticating of the ~~said~~ user information indicates the ~~said~~ user information is invalid, blocking all traffic on the ~~said~~ port except for packets related to a user authentication protocol;

if the ~~said~~ authenticating of the ~~said~~ user information indicates the ~~said~~ user information is valid, determining whether the ~~said~~ user is associated with a VLAN supported by the ~~said~~ network access device by receiving a message from an authentication server, wherein the ~~said~~ message comprises a VLAN identifier (ID) associated with the ~~said~~ user information;

if the ~~said~~ user is not associated with the ~~said~~ VLAN,

assigning the ~~said~~ one of the ~~said~~ plurality of input ports to a port default VLAN; and

blocking all traffic on the ~~said~~ one of the ~~said~~ plurality of input ports except for packets related to the ~~said~~ user authentication protocol; and

if the ~~said~~ user is associated with the ~~said~~ VLAN,

assigning the ~~said~~ one of the ~~said~~ plurality of ports to the ~~said~~ VLAN associated with the ~~said~~ user; and

restricting access to the ~~said~~ one of the ~~said~~ plurality of input ports in accordance with a user policy associated with the ~~said~~ user information.

41. (Currently Amended) The method of claim 40, wherein the ~~said~~ network switch comprises a layer 2 network access device.

42. (Currently Amended) A network system, comprising:

a data communications network;

a network access device coupled to the ~~said~~ data communications network; and

a user device coupled to a port of the ~~said~~ network switch, wherein the ~~said~~ network access device is adapted to:

authenticate a physical address of a user device coupled to one of the ~~said~~ plurality of input ports;

drop packets from the ~~said~~ user device if the ~~said~~ physical address is invalid;

authenticate user information provided by a user of the ~~said~~ device only if the ~~said~~ physical address is valid;

if authentication of the ~~said~~ user information indicates the ~~said~~ user information is invalid, block all traffic on the ~~said~~ one of the ~~said~~ plurality of input ports except for packets related to a user authentication protocol;

if authentication of user information indicates the ~~said~~ user information is valid, determine whether the ~~said~~ user is associated with a VLAN supported by the ~~said~~ network access device by receiving a message from an authentication server, wherein the ~~said~~ message comprises a VLAN identifier (ID) associated with the ~~said~~ user information;

if the ~~said~~ user is not associated with the ~~said~~ VLAN,

assign the ~~said~~ one of the ~~said~~ plurality of input ports to a port default VLAN; and

block all traffic on the ~~said~~ one of the ~~said~~ plurality of input ports except for packets related to the ~~said~~ user authentication protocol; and

if the ~~said~~ user is associated with the ~~said~~ VLAN,

assign the ~~said~~ one of the ~~said~~ plurality of ports to the ~~said~~ VLAN associated with the ~~said~~ user; and

restrict access to the ~~said~~ one of the ~~said~~ plurality of input ports in accordance with a user policy associated with the ~~said~~ user information.

43. (Currently Amended) The network system of claim 42, wherein the ~~said~~ network access device comprises a layer 2 network access device.

44. (Currently Amended) The device of Claim 1 wherein the ~~said~~ user information comprises a user name and a password.

45. (Currently Amended) The method of Claim 13 wherein the ~~said~~ user information comprises a user name and a password.

46. (Currently Amended) The system of Claim 23 wherein the ~~said~~ user information comprises a user name and a password.